INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET EN AUTOMATIQUE

Localization and Routing In Multihops Wireless Access Networks

Fabrice Theoleyre — Fabrice Valois

N° 5461

Janvier 2005

THÈME 1

Rapport de recherche

ISSN 0249-6399 ISRN INRIA/RR--5461--FR+ENG

Localization and Routing In Multihops Wireless Access Networks

Fabrice Theoleyre * , Fabrice Valois†

Thème 1 — Réseaux et systèmes
Projet ARÈS

Rapport de recherche n° 5461 — Janvier 2005 — 15 pages

Abstract: Multihops Wireless Access Networks are ad hoc networks connected to Internet through wireless Access Points. They constitute a logical extension of cellular wireless networks to extend the radio covering area in a spontaneous manner in introducing a collaboration among the nodes. They propose a flexible and cheap infrastructure. A client can be contacted and can contact any other host in the Internet. To reach this goal, we propose a solution of micro-mobility management and routing for such hybrid network. This solution uses a virtual backbone collecting the control traffic and minimizing overheads. The mobility management combines both proactive and reactive approach to propose a trade-off between overheads and delays. When a packet arrives from Internet to the AP, the mobile destination is localized in a reactive way. Inversely, a mobile can initiate a communication to the Internet with a proactive solution, without latency. Some mechanisms of route maintenance without any additional overhead are also proposed.

Key-words: ad hoc networks, hybrid networks, routing, localization, mobility management, virtual structure

* Laboratoire CITI, INSA Lyon – INRIA ARES – fabrice.theoleyre@insa-lyon.fr
† Laboratoire CITI, INSA Lyon – INRIA ARES – fabrice.valois@insa-lyon.fr

Unité de recherche INRIA Rhône-Alpes
655, avenue de l'Europe, 38334 Montbonnot Saint Ismier (France)
Téléphone : +33 4 76 61 52 00 — Télécopie +33 4 76 61 52 52

Localisation et Routage dans les réseaux d'accès sans fil multisauts

Résumé : Les réseaux d'accès sans fil multisauts sont des réseaux ad hoc connectés à Internet via un ou plusieurs Point d'Accès. Ils constituent une prolongation logique des réseaux cellulaires en étendant la couverture radio de façon spontanée, introduisant une collaboration parmi les noeuds. Ils proposent une infrastructure réseau flexible et bon marché. Un noeud peut contacter et être contacté par n'importe quel hôte de l'Internet. Dans ce but, nous proposons une solution de gestion de la micro-mobilité et de routage au sein d'un réseau hybride. Cette solution utilise une dorsale virtuelle afin de collecter le trafic de contrôle et donc de minimiser l'overhead induit. Elle combine à la fois une approche proactive et réactive dans le but de proposer un compromis entre l'overhead et le délai de bout en bout. Lorsqu'un paquet arrive d'Internet, l'AP localise réactivement la destination au sein de la zone ad hoc. Inversement, un mobile peut initier proactivement une communication vers Internet, sans latence. Des mécanismes de maintenance de route sans ajout d'overhead sont également proposés.

Mots-clés : réseaux adhoc, réseaux hybrides, routage, localisation, gestion de la mobilité, structure virtuelle

1 Introduction

Mobile Ad Hoc networks (MANets) could be defined by *spontaneous wireless networks*: some nodes communicate with each other, via wireless transmissions, and collaborate to set up an efficient network, without the help of wireless or wired routers. All nodes are both clients and routers. Multihops Wireless Access Networks (or hybrid networks) are such a MANET connected to the Internet via special gateways: the Access Points (AP). The key problem in this network is to exchange information between the Internet and the ad hoc network. We assume that the nodes in an hybrid network will mainly communicate with the Internet, and not necessarily with other clients of the ad hoc network where classical MANET routing solutions (AODV, OLSR...) are appropriate. The hybrid networks could be useful in several environments: an operator could inexpensively extend its cellular networks, a university could propose a complete cover of its campus, allowing students to access to a central mail or file server.

We propose to create a routing solution for hybrid networks and to provide a proactive localization for important nodes. Many articles deal with the problem of routing in MANets, with a proactive ([3]) or reactive ([6]) approach. But, just a few articles propose a routing solution specific to hybrid networks ; moreover some weaknesses remain. Indeed, routing optimizations are not the same, because we reduce the number of potential destinations, the AP can act as network manager... We want to set up a localization process like in cellular networks (GSM, GPRS...). To communicate, a mobile can register its location in the gateway serving its area, or oppositely, the cellular network can initiate a paging to determine the location of a particular mobile when a packet intended to it arrives. We want to adapt such a solution to a multihops wireless access network.

In [12], we proposed a protocol constructing and maintaining a virtual dynamic backbone. This backbone elects stronger nodes in the hybrid network to act as routers and managers, the root of the backbone being the AP. This backbone can optimize flooding in creating a structure collecting the control traffic and reducing the load for other nodes. Our routing solution uses this virtual backbone. More precisely, it is used for flooding `Route Requests`, useful to discover a route to a mobile node from the AP when packet comes from the Internet. The clients of the backbone don't take part in this process, sparing their energy and reducing the global overhead. Moreover, this backbone constitutes a tree, rooted at the AP. In this way, it could help us to optimize the communications from a client to the Internet, proposing a proactive knowledge for routing without additional overhead. Then, the delay is reduced comparing to a reactive approach. In conclusion, the AP could act as a Mobile IP - Foreign Agent [9] to manage the macro mobility, and our routing protocol could manage the micro mobility, inside the ad hoc network. Extended solution of our virtual backbone [11] provides more robustness and reliability according to multipath topology and multiple AP.

Next, we will expose related works about routing solutions in hybrid and cellular networks. Section 3 describes our routing and localization solution, and gives some elements of comparison and differences with cellular networks. Section 4 gives simulation results about the overheads, delays and delivery ratios. Finally, section 5 exposes some perspectives.

2 Related Work

2.1 Cellular networks

There exist several solutions to handle mobility in cellular networks: a node can change its AP with a minimized delay and overhead, maintaining a good delivery ratio. Usually, we separate the micro and the macro mobility. Mobile IP [9] is commonly used to manage mobility through several different access networks, and another protocol is used to reduce overheads in managing locally the location of its clients. Cellular IP [2], for example, creates a hierarchy between access routers, forming a tree with the *Gateway* representing the root. A client updates its location by sending a `Route Update` toward the *Gateway*. Each intermediary router updates its cache in inscribing the next hop toward the source, creating a route. However, such solutions could not be applied in hybrid networks: we have no backbone, no specialized routers and communications between the AP and a client could be multihops.

2.2 Hybrid networks

Some articles deal with the problem of routing in hybrid networks. MIPMANET [7] proposes to integrate AODV and Mobile IP. AODV is used for internal communications. For external communications, the node registers itself to the Foreign Agent (FA). The FA is an ad hoc node like other nodes. For upload, the packet is forwarded to the FA. For download, the packet follows the classical route of Mobile IP, from the *Corresponding Node* to the *Foreign Agent*, and eventually via the *Home Agent*. Finally, the FA delivers the packet to the ad hoc node, with the routing procedure of AODV. However, this solution presents some weaknesses. A node must send multiple `Route Requests` before deciding the destination is in the Internet without being certain because of the broadcast storm problem [8]. Moreover, the FA must periodically flood the network with `Mobile IP advertisements`. We find the integration of multiple AP allowing handover problematic. Finally, this solution supposes that the ratio of internal communications is sufficient to justify the additional overhead. [1, 10] present a similar approach. [10] presents some improvements about the advertisements, proposing a reactive approach combined to the proactive solution. However, we assume the trade-off complex to parameterize, and the overhead remains high for the AP discovering. [5] presents a study of performance evaluation of the previous solution. The delivering delays remain high: more than 1 seconds whatever the solution is proactive or reactive. The delivery ratio is also a quite low: 86% for 4 APs and 12.5 nodes per AP, which represents almost only single hops wireless communications.

To the best of our knowledge, only MEWLANA [4] proposes an optimized solution for hybrid networks. MEWLANA-TD optimizes internal communications and allows packets exchange with the Internet. It is inspired from MIPMANET and it integrates Mobile IP and a proactive routing protocol (DSDV). Hence, we assume that this solution presents the same drawbacks as MIPMANET. In MEWLANA-RD, the AP sends periodically `Agent advertisements`. Each node forwards the packet and registers the previous hop as next

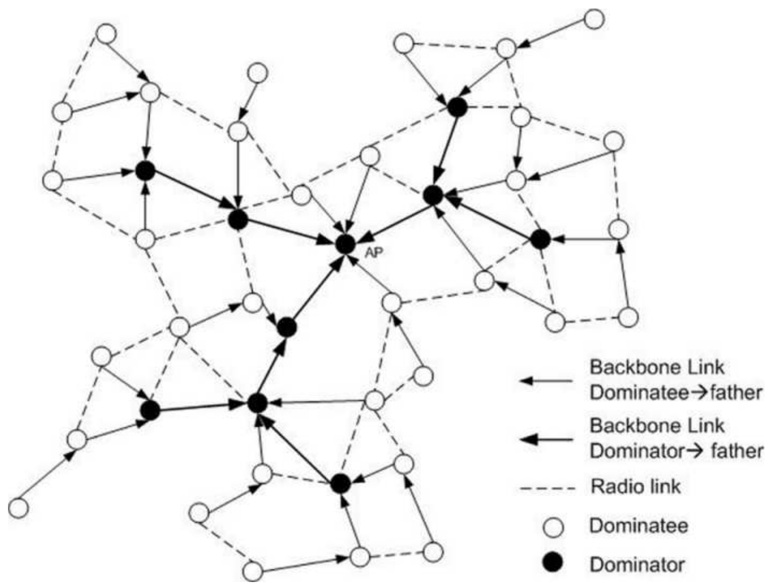

Figure 1: An example of our virtual backbone (2-CDS)

hop toward the AP, which constitutes the default route. Simultaneously, it registers itself in unicast to the AP, using this inverse route, and creating an inverse entry for it in each intermediary nodes. Finally, MEWLANA-RD creates a bidirectional tree with the AP representing the root. The AP knows proactively a route toward each node, and each client knows a route toward its AP. The authors prove that MEWLANA-RD outperforms MIP-MANET for an access network. However, we assume that the periodic reconstruction of the tree creates an important overhead. Collisions are more frequent, perturbing the data traffic.

3 Proposition

Our solution mainly focus on the problem of routing toward and from the Internet. The AP must know the location of its clients in the ad hoc area to route them data packets. We must optimize overhead, robustness and latency for the creation of a route, the delivery ratio for data flows. We want to adapt an efficient solution in cellular networks: *Cellular IP*. To achieve this goal, we use a virtual backbone, the backbone members acting as routers. This backbone helps us to optimize the flooding. However, we must adapt *Cellular IP* to take into account the self constraints of hybrid networks: limited bandwidth, frequent backbone changes because of maintenance, energy management…

3.1 Backbone

We use the virtual dynamic backbone presented in [12]. This solution selects stronger nodes to act as backbone members, the *dominators*. These dominators are elected according to their weight, representing their *capacity* to act as network leaders. Our solution is based on the knowledge of the k_{cds}-neighborhood. Currently, each node sends the list of its neighbors k_{cds}-1 hops far. Some nodes are elected to act as *dominators*, to form a connected structure, where each *normal* node, the *dominatees*, is at most k_{cds} hops far from at least one dominator: it represents a k_{cds}-CDS. The backbone constitutes a tree of *dominators*, with *dominatees* representing the leaves (fig. 1 represents a 2-CDS). Each node except the AP (the root) owns a parent, hierarchical superior in the tree. Symmetrically, each dominator maintains the identity of the dominators for which it is a parent: they constitute its *children*.

MANET constitute volatile environments. Hence, we proposed a maintenance protocol to maintain the efficiency of the backbone. To maintain the backbone connectivity, the AP sends periodically `AP-hellos`. These packets could integrate similar information to `Mobile-IP advertisements` for the Internet access. The `AP Hellos` are only forwarded by the *dominators*, reducing the overhead comparing to the classical flooding of `Agent advertisements` from MEWLANA-RD. The *dominatees*, don't participate to the backbone maintenance, so they can spare their energy.

In conclusion, our backbone, thanks to the k_{cds}, has a parameterizable cardinality. An high k_{cds} allows many nodes to spare their energy in not participating in the network management, but the backbone is less stable, and the proactive knowledge of the k_{cds}-Neighborhood creates an important overhead. A small k_{cds} is suited for very mobile environments, and an high k_{cds} for almost static networks.

3.2 Route to the Internet

A node is allowed to initiate a communication to the Internet. Hence, it must have a route toward an AP. The AP can represent the default route for unknown destinations. The backbone topology is very useful for such a goal. The backbone forms a tree, the AP being the root. Moreover, each node owns a *parent*. For a dominatee, the *parent* is the node representing its principal dominator, the intermediary node to contact the backbone. For the dominators, the parent is the dominator from which it receives the `AP hellos`, so it is the next hop toward the AP, via other dominators. This information is necessary for the backbone maintenance process.

Hence, each node owns already a default route to the AP, through its parent. Moreover, this default route is proactive. We assume that each node must probably communicate with the AP: for a *Mobile IP registration*, to send data to the Internet... Hence, a proactive knowledge is useful since it reduces significantly the delay and the overhead because of the lack of `Route Request` floodings. With the information provided by the virtual backbone, the route construction has no cost, no overhead and no latency.

3.3 Route from the Internet

The AP must know an inverse route when a packet comes from the Internet, and it must forward this packet to the destination in the ad hoc network. We assume that a communication is mainly initiated by a node in the ad hoc area. Moreover, in this part, we describe a solution to create inverse route automatically when the communication is initiated by a node in the ad hoc area. Hence, we think a reactive approach efficient, because this route discovering will occur seldom. Our solution could be compared to the paging mechanism in cellular networks: the *Base Stations* must find reactively the location of a mobile when a data packet arrives.

When the AP receives a packet to forward, and no route is known to the destination, it engages the following procedure:

- The AP buffers the packet until a route is known. It creates a `Route Request` and sends it to its children in multicast. The multicast address corresponds to a backbone flooding from the root toward the leaves.
- Each dominator which receives the request searches if the destination is in its neighborhood table:
  - If the destination is not one of its dominatee, the dominator forward the `Route Request` in multicast to its children
  - If the destination is one of its dominatees (it is registered as parent for this node in the neighborhood table), it creates a `Route Reply` and sends it to its parent, in unicast. The dominator acts as a proxy to create a `Route Reply`. Thus, we spare on average $\frac{2 \cdot k_{cds}}{2}$ radio transmissions (to and from this dominatee).

The environment is mobile, and the backbone is continuously maintained. However, some dominatees can be sometimes disconnected from the backbone. A dominatee must realize that its dominator is gone, search a new parent, and enter in election process if it doesn't find any new potential parent. To decrease the effect of such disconnection, when a dominator receives a `Route Request` for a destination in its neighborhood table, this destination having no parent, it initiates a `Route Reply`. Hence, a `Route Request` can sometimes but rarely generate several `Route Reply`. Only the *dominators* forward the `Route Request`, optimizing the overhead.

The `Route Reply` follows the inverse route of the `Route Request`. However, the route doesn't need to be accumulated in the `route Request`. Each dominator just forwards the `Route Reply` to its parent, until the packet reaches the AP. Each relay simultaneously registers an inverse route, associating the source of the `Route Reply` and the dominator from which the `Route Reply` comes. We create a local routing table. Hence, if another source needs to send a data packet to the same destination, a route is already known. We use this mechanism for internal routing optimizations (section 3.4).

It could be interesting to maintain proactively the route for specific nodes. This could be useful when a node has an important role in the ad hoc network (file sharing...), or if the node is in communication, doesn't need to send some data packets, but it waits for other packets from the Internet. To maintain proactively a route, a node can send periodically `Route Update`, acting like a gratuitous `Route Reply`. The latency for the route discovering is deleted. `Route Updates` are unicast packets, having a small impact on overhead.

We propose a gratuitous mechanism to refresh routes, like in *Cellular IP*. When a node forwards a data packet, it refreshes in its routing table the timer associated to the source of the packet. The communications being often bidirectional, when the node initiates a communication to the Internet, no `Route Request` is needed for the answer of the server. Moreover, when a dominatee changes its parent, it just needs to send a data packet to refresh the route along the whole backbone. In this way, we reduce the overhead to maintain routes.

During maintenance, a dominator can choose to change its parent, and reconnect itself to another part of the backbone, creating obsolete routes for all its branch. A dominator which remarks that one of its child is gone, deletes all the routes passing through this child. Then, it sends a `Route Delete` to advertise its decision to its hierarchy. Hence, the obsolete routes are deleted. When the AP will receive a packet for a node of this branch, it will initiate a new route discovering, and won't use the obsolete route.

We can integrate several AP in the hybrid network to create a reliable Internet access and a load balancing among the AP. We propose to create one backbone per AP. Each AP sends periodically `AP hello`, integrating the additional parameters required for the Internet access: Mobile IP parameters, address prefix...In the future, the AP will constitute in hybrid networks a Service Central Point for mobility management, billing...With the `AP Hellos`, we have several backbones, representing a multihops covering area for each AP. A dominator in changing its parent, can also do an handover for its branch, gather the Internet access parameters from its new parent, and distribute this information to all its branch in multicast. We assume such a solution is efficient.

3.4 Optimizations for Intern Communications

We want to optimize external communications, but allowing the possibility to bypass the AP for internal communications. We propose a solution, with delays and route lengths which are not optimal, but this type of communications doesn't prevail.

When S want to contact D, it doesn't know if D is in the ad hoc network or in the Internet. However, we want to avoid the flooding of the ad hoc network. Hence, S searches if a route to D is known locally, in the routing table, or directly in the neighborhood table. If right, the data packet is directly sent to D, via the corresponding route. Else, S forwards the data packet to its parent P. Then, P executes the same procedure. Recursively, if no route is known in the ad hoc network, the data packet will arrive to the AP. If the AP doesn't known any route, it can test if the destination is in the ad hoc area or in the Internet (for example thanks to the address prefix). If it is an ad hoc node, it will buffer the packet and send a `Route Request` to the ad hoc area. When we `Route Reply` is received, the AP can send the data packet via this new route.

If S or another node want further to contact the same destination D, a route is already known. Thus, the data packet won't probably reach the root. It will be automatically forwarded to D when the packet arrives to a dominator which is aware of the route. The length in such a scheme is not optimal: the data packet is forwarded toward the ancestor in common with S and D. However, it is not our goal, currently, to optimize such a scenario.

4 Performance Evaluation

4.1 Simulation

We simulate our proposition using Opnet Modeler 8.1. We use the implementation of the 802.11b radio model provided by Opnet with a radio range of 300m. We use the random waypoint mobility model to simulate the nodes trajectories on a square area, the surface depending on the degree. The default parameters are 40 nodes, a speed of 5 m.s^{-1} and a degree of 10. To stress our solution, we use short communications and change frequently the source and destination. Thus, a source sends a flow of 8 data packets to the AP. The packets have a length of 128 octets. In a flow, each packet is sent every 0.25 seconds. The flow interarrival process follow an exponential distribution with a mean of 2 seconds. The number of simultaneous communicating nodes appears to be a parameter of the simulation. We suppose the traffic as symmetric. Thus, the AP sends data flows according to the same process to a random destination. At the end of a flow packet, the source is changed according to a random process. We use the backbone described in [12], with a k_{cds}=2: this means that a node is at most 2 hops far from the backbone.

To evaluate our proposition, we investigate the behavior of the localization and routing protocol in the case of communications between the ad hoc network and the Internet. The performance evaluation parameters are mainly (1) the end-to-end delay between the source and the destination *i.e.* the average delay between the time of the data packet generation, and the reception time at the destination, (2) the delivery ratio. We study the impact of the mobility, the number of nodes and connections. We also compute the different overheads for each part of the protocol. Finally, we have also implemented MEWLANA-RD in order to compare with our proposition, since it outperforms MIPMANET for external communications. MEWLANA-RD must use a neighborhood discovering, necessary for the detection of unidirectional links.

4.2 Results

4.2.1 Mobility

Figure 2 shows the impact of node speed on the end to end delay. Our proposition (label 'cdcl') is robust according to a high variation of node dynamicity. More, the delivery time is symmetric (in download and in upload). A packet is delivered in less than 15ms, whatever the speed. MEWLANA-RD, which is a complete proactive approach, presents the same delay. Thus, our hybrid solution combining a reactive and a proactive approach, doesn't increase the delay for the route discovering. The mean path in our solution (2.7 hops) is a little higher than for MEWLANA-RD (2.64 hops). Our solution uses a virtual backbone

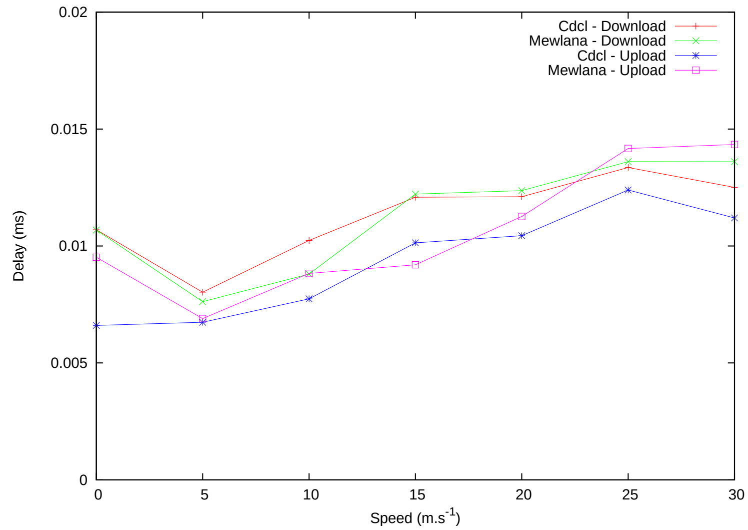

Figure 2: End to End Delay According to the Mobility

to reduce the complexity and the dynamicity of the physical topology. Hence, we create a small route lengthening. However, this little increase (2.3%) seems largely acceptable. Thus the maintenance of a virtual structure seem better than a periodical reconstruction.

Figure 3 illustrates the impact of low and high mobility on the packet delivery ratio. MEWLANA-RD offers a non symmetric results: upload operation have a better performance than download one. Our solution is more homogeneous. For a reasonable node speed (about $10m.s^1$), 97% of packets are delivered.

4.2.2 Impact of number of nodes

Figures 4 and 5 illustrate the robustness and reliability of data transmission between ad hoc and IP networks. Our solution presents a very high delivery ratio, almost constant. MEWLANA-RD loses more data packets, and suffers more from the increasing of the network cardinality. Naturally, when we have more nodes in the network, the delivery ratio decreases and the delivery time increases. Since we increase the number of nodes and maintain the degree constant, the route length increases, increasing the delivery time too.

4.2.3 Impact of number of couples Source/Destination

Figure 6 illustrates also the robustness and the reliability of data transmission but according to the number of active nodes or sources. Our solution delivers 10% of data packets more than MEWLANA-RD, with almost the same delay. It is also interesting to highlight that

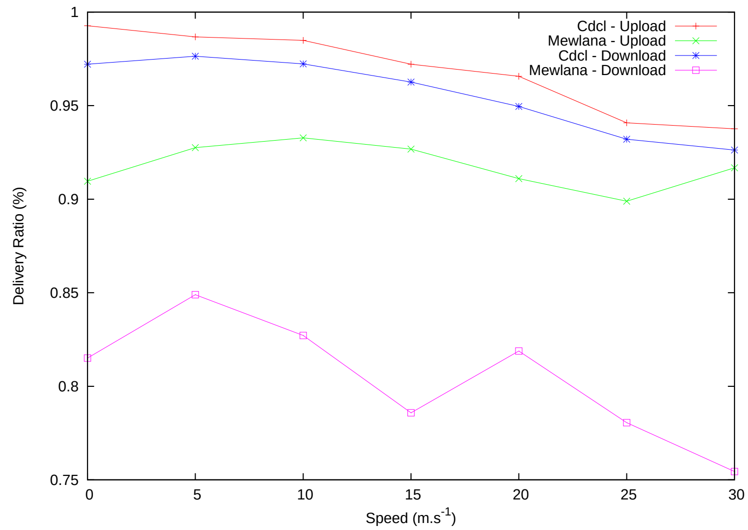

Figure 3: Delivery Ratio according to the Mobility

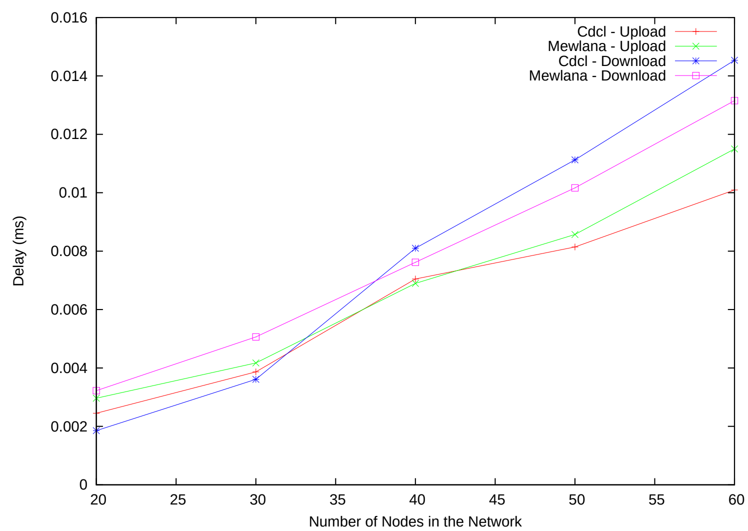

Figure 4: End to End Delay According to the number of Nodes in the Network

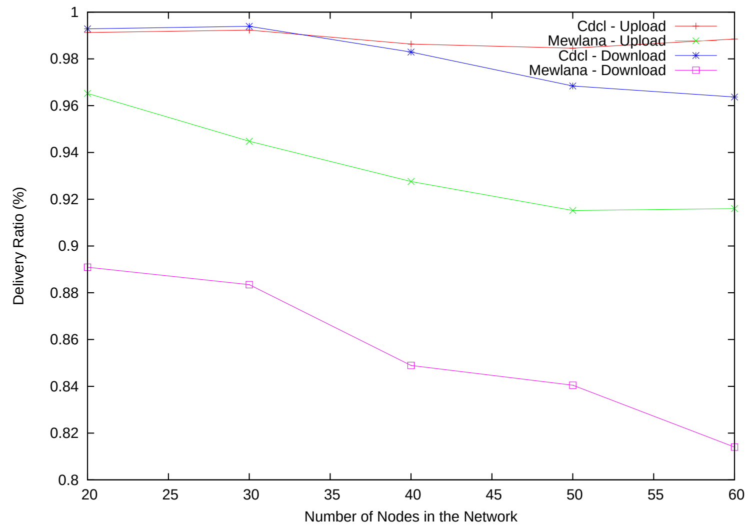

Figure 5: Delivery Ratio according to the number of Nodes in the Network

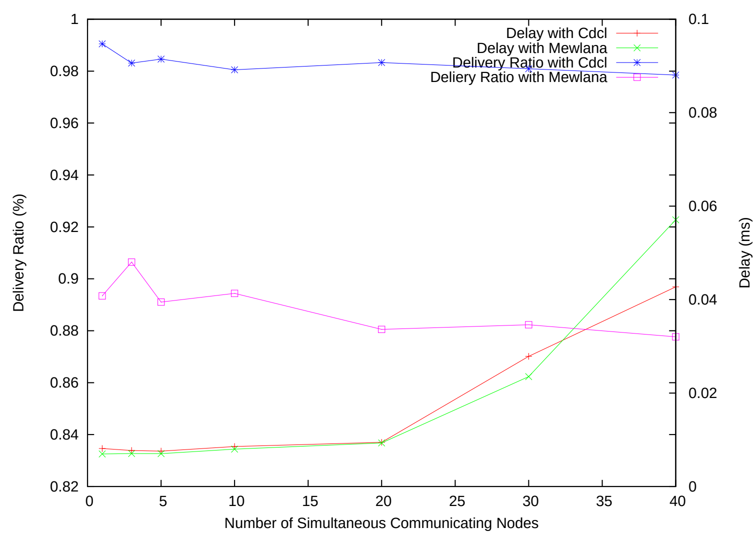

Figure 6: Delivery Ratio and Delay according to the number of simultaneous Communicating Nodes

both solutions are robust: the performance results are slightly insensitive to the increasing of the number of active nodes.

	Cdcl	MEWLANA-RD
Hellos	0.32	0.25
Data	0.3	0.28
Data retransmissions	0.01	0
Acks	0.26	0.35
AP Hellos	-	0.25
AP Registrations	-	0.58
Route Request	0.01	-
Route Reply	0.0043	-
Route Delete	0.005	-
Virtual Topology	0.165	-
Overhead Total	0.761	1.074

Table 1: Overheads (in packets per node per second)

4.2.4 Overheads

Tab. 1 presents the different overheads of our solution and of MEWLANA-RD. All packet types are detailed. We can see that our virtual topology is efficient in reducing the overhead for localization, the `Route Request`, `Route Delete` and `Route Update` using the backbone. MEWLANA-RD which continuously reconstructs its backbone present a very high overhead, this overhead being almost 40% higher. Moreover, MEWLANA-RD suffers from a high broadcast overhead, creating collisions, and the protocols suffers from its lack of reliability.

4.2.5 Intern Routing

The main objective of our solution is to provide an optimized routing solution between the ad hoc area and the Internet. But as an optimization, our solution could provide an ad hoc connectivity, with internal routing. Fig. 7 presents the delivery ratio and delay according to the *intern communications ratio*, i.e. the ratio of communications initiated by nodes toward another node not Access Point to the total number of communications. Because we allow internal communications, the routes are, on average, longer (2.16 hops on average with uniquely extern communications, and 2.6 hops on average for uniquely intern communications). However, both delivery ratio and delay are almost constant according to the *intern communications ratio*. Our solution presents good performances, even with our internal routing process.

5 Conclusion

We propose a routing solution optimizing the communications between the hybrid network and the Internet, using a virtual backbone to collect control traffic and to optimize the overhead. In upload, we use the information of the backbone maintenance: our routing

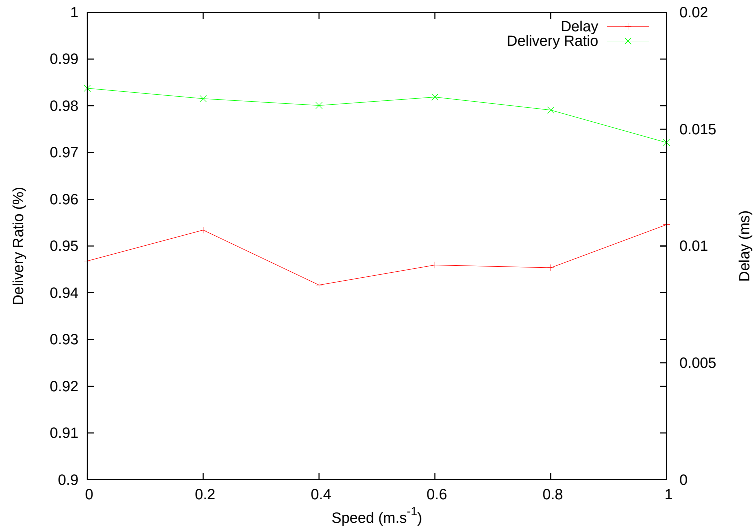

Figure 7: Delivery Ratio and Delay for The Intern Routing

solution is proactive and doesn't present any additional overhead or latency. In download, our solution is reactive to discover a route, with a maintenance protocol sending `Route Delete` and `Route Update` to update and delete obsolete routes. Our solution delivers on average 70% of the data packets with acceptable delay and overhead, and supports several simultaneous communications. Finally, we propose a solution to allow routing inside the ad hoc area, without passing through the AP. The solution presented in [11] allows the integration of several backbones and AP. Thus, our hybrid network could naturally be managed by multiple gateways. The virtual structure hides a part of the mobility to higher levels, in proposing a backbone constituting a simple logical view of the hybrid network. Next step of this study will be the implementation of new functions like the paging, the handover with the choice of the optimal AP, a sleeping mode, an address assignment service... The implementation of a multicast routing protocol using the particular form of tree of our backbone could be studied. In the future, our virtual dynamic backbone will constitute a framework for easier services deployment.

Thanks to: Olivier Schirmann and Maryline Loscos for their participation, and suggestions in the implementation of this solution.

References

[1] E Belding-Royer and Yuan Sun. Connectivity for ipv4 mobile ad hoc networks. Internet-Draft Version 00, IETF, November 2001.

[2] Andrew Campbell, Javier Gomez, Chieh-Yih Wan, and Sanghyo Kim. Cellular ip. Internet-Draft Version 01, IETF, december 2000.

[3] Thomas Clausen, Philippe Jacquet, Anis Laouiti, Pascale Minet, Paul Muhlethaler, Amir Qayyum, and Laurent Viennot. Optimized link state routing protocol (olsr). Internet draft version 07, IETF, November 2002.

[4] Mustafa Ergen and Anuj Puri. Mewlana-mobile ip enriched wireless local area network architecture. In *56th Vehicular Technology Conference*, Vancouver, Canada, September 2002. IEEE.

[5] Mona Ghassemian, Philipp Hofmann, Christian Prehofer, Vasilis Friderikos, and Hamid Aghavami. Performance analysis of internet gateway disocvery protocols in ad hoc networks. In *Wireless Communications and Networking Conference*, Atlanta, USA, March 2004. IEEE.

[6] David B Johnson and David A Maltz. Dynamic source routing in ad hoc wireless networks. In Imielinski and Korth, editors, *Mobile Computing*, chapter 5, pages 153–181. Kluwer Academic Publishers, 1996.

[7] Ulf Jonsson, Fredrik Alriksson, Tony Larsson, Per Johansson, and Gerald Q. Maguire. Mipmanet - mobile ip for mobile ad hoc networks. In *Proceedings of the first ACM international symposium on Mobile and ad hoc networking and computing*, pages 75–85, Boston, Massachusetts, USA, May 2000. ACM, IEEE Press.

[8] S.Y. Ni, Y.C. Tseng, Y.S. Chen, and J.P. Sheu. The broadcast storm problem in a mobile ad hoc network. In *MobiCom*, pages 151–162, Seattle, USA, August 1999. ACM.

[9] Charles Perkins. Ip mobility support for ipv4. Internet-Standard rfc 3344, IETF, August 2002.

[10] Yuan Sun, Elizabeth M. Belding-Royer, and Charles E. Perkins. Internet connectivity for ad hoc mobile networks. *International Journal of Wireless Information Networks*, 9(2), April 2002.

[11] Fabrice Theoleyre and Fabrice Valois. Robustness and reliability for virtual topologies in wireless multihops access networks. In *Mediterranean Ad Hoc Networking Workshop*, Bodrum, Turkey, June 2004.

[12] Fabrice Theoleyre and Fabrice Valois. A virtual structure for mobility management in hybrid networks. In *Wireless Communications and Networking Conference (WCNC)*, pages 1035–1040, Atlanta, USA, March 2004. IEEE.

Unité de recherche INRIA Rhône-Alpes
655, avenue de l'Europe - 38334 Montbonnot Saint-Ismier (France)

Unité de recherche INRIA Futurs : Parc Club Orsay Université - ZAC des Vignes
4, rue Jacques Monod - 91893 ORSAY Cedex (France)
Unité de recherche INRIA Lorraine : LORIA, Technopôle de Nancy-Brabois - Campus scientifique
615, rue du Jardin Botanique - BP 101 - 54602 Villers-lès-Nancy Cedex (France)
Unité de recherche INRIA Rennes : IRISA, Campus universitaire de Beaulieu - 35042 Rennes Cedex (France)
Unité de recherche INRIA Rocquencourt : Domaine de Voluceau - Rocquencourt - BP 105 - 78153 Le Chesnay Cedex (France)
Unité de recherche INRIA Sophia Antipolis : 2004, route des Lucioles - BP 93 - 06902 Sophia Antipolis Cedex (France)

Éditeur
INRIA - Domaine de Voluceau - Rocquencourt, BP 105 - 78153 Le Chesnay Cedex (France)
http://www.inria.fr
ISSN 0249-6399